

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

JANE DOE on behalf of herself and :
others similarly situated, : Case No.

Plaintiff, :

v. :

THE UNIVERSITY OF MICHIGAN :
BOARD OF REGENTS, KEFFER :
DEVELOPMENT SERVICES, LLC, :
and MATTHEW WEISS. :

Defendants.

/

CLASS ACTION COMPLAINT AND JURY DEMAND

INTRODUCTION

1. Plaintiff and the class are current and former student athletes and victims of the data breach on the University of Michigan and Keffer Development Services' databases, exposing their highly sensitive personally identifiable information and medical records to a sexual predator, Matthew Weiss. The breach continued for nearly a decade because the University and Keffer failed to prevent, detect, or stop Weiss from accessing those databases without authorization, allowing him to download the private sensitive information belonging to 150,000 student athletes from over 100 colleges and universities.

2. With that information, Weiss then targeted individual athletes' personal accounts and built dossiers on thousands of young women, downloading their private photos and making notes on their bodies and sexual preferences.

3. This egregious and devastating breach was entirely preventable by the University and Keffer. As noted in a criminal complaint by the United States Attorney in the Eastern District of Michigan, Weiss breached the University and Keffer's systems using *only* compromised credentials belonging to University employees. This is because, on information and belief, neither the University nor Keffer required that its employees implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personally identifiable information, especially medical information. Nor did the University or Keffer implement reasonable security measures to ensure that only authorized individuals could access student PHI.

4. HIPAA and Michigan state law require entities collecting medical information to secure it using reasonable means. Indeed, the University and Keffer recognized those duties under their policies, with Keffer representing that it uses "industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction

or modification.”¹ But despite that promise, Keffer never implemented adequate safeguards, leaving students’ PHI an unguarded target for predators like Weiss.

5. The University and Keffer thus violated their duties to the student athletes under tort, contract, and statutory law, rendering them liable to Plaintiff and the class for the harm this devastating invasion of privacy caused.

PARTIES

6. Plaintiff Jane Doe is a former student athlete at the University of Michigan, and citizen of Texas, where she intends to remain.

7. Defendant, the Regents of the University of Michigan (“the University”), is the entity that governs the University of Michigan. Mich. Comp. Laws §§ 390.3 and 390.4.

8. Defendant, Keffer Development Services, LLC, is a technology vendor operating the electronic medical record system known as “The Athletic Trainer System.” Keffer is headquartered in Grove City, Pennsylvania, and continuously does business in Michigan, as described below, availing it of the protections of Michigan state law. Keffer is a domestic LLC in Pennsylvania.

9. Defendant, Matthew Weiss, is an individual and citizen of Michigan.

¹ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf.

JURISDICTION & VENUE

10. This Court has subject matter jurisdiction under 28 USC § 1332(d) because this is a class action in which the amount in controversy exceeds \$5,000,000, there are more than 100 class members, and the majority of class members are citizens of different states than defendants.

11. This Court also has jurisdiction under 28 USC §§ 1331 and 1367 because Plaintiff alleges a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) et seq., and supplemental jurisdiction over additional related claims under 28 U.S.C. § 1337(a).

12. Plaintiff is also timely filing a Notice of Intent to File Claims in the Court of Claims under MCL 600.6431.

BACKGROUND

Keffer Development Services

13. Keffer is a software vendor that developed the electronic medical record system known as The Athletic Trainer System or “ATS.”

14. The ATS program is designed to store the “protected health information” belonging to students, including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight.

15. Keffer's operations span the country, including at the University and over 100 colleges and universities. In total, Keffer has collected the PHI belonging to over 150,000 college athletes at those institutions.

16. In collecting this information, Keffer knows it has an obligation to protect it under state and federal law.

17. Its internal policies recognize this obligation:

Keffer Development Services, LLC Privacy Policy

Last updated: July 2, 2024

Keffer Development Services, LLC. ("KDS") is committed to maintaining the security and privacy of

personal information collected through this website, www.atsusers.com (the "Website"), the KDS electronic health record (the "EMR") and the various KDS portals (the "Athlete Portals"). This Privacy Policy discloses KDS' information collection and dissemination practices in connection with the Website, the EMR and the Athlete Portals and applies solely to the information that we collect through those means. This Privacy Policy does not address personal information that you provide to us in other contexts (e.g., through another relationship not expressly described in this Privacy Policy).

Security

KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.

18. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' PHI.

19. As one example, while Keffer maintained the option to incorporate multi-factor authentication to access its ATS applications, on information and belief, it did not *require* that institutions and users do so. That security failure proved critical, as Weiss gained access to student PHI with only the access credentials belonging to other administrators and users.

20. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long breach at issue here.

The University of Michigan

21. The University is an elite-level state institution enrolling students from across the country, including in its athletics programs.

22. In so doing, the University provides its student athletes medical treatment, including from athletic trainers employed by the University.

23. To facilitate that treatment, the University contracted with Keffer to use the ATS application over web and mobile devices.

24. When collecting that information, the University, like Keffer, accepted an obligation to protect it under contract and statutory principles, including under HIPAA.

25. The University, in turn, recognizes the obligation to protect that information under University policy:



How We Secure Your Information

The U-M recognizes the importance of maintaining the security of the information it collects and maintains, and we endeavor to protect information from unauthorized access and damage. The U-M strives to ensure reasonable security measures are in place, including physical, administrative, and technical safeguards to protect your personal information.

26. However, like Keffer, the University failed to implement the security measures needed to fulfill that promise, including staff training on securing credentials, requiring MFA to use the ATS system, and monitoring and auditing access to student files.

27. Nor did the University ensure Keffer had adequate security measures in place to protect its students' PHI from theft and misuse.

28. Indeed, the University lacked adequate training programs to detect and stop breaches like those caused by Weiss.

29. The University and Keffer breached their duties, allowing Weiss to steal the medical and personal records belonging to thousands of students, including sensitive photos and treatment information.

30. Because Keffer and the University failed to implement basic, industry standard security measures, they allowed a predator, ex-football coach Matthew Weiss, to access University students' most sensitive information for nearly a decade.

31. From 2015 to 2023, Weiss gained access to student files within the ATS app using only the access credentials belonging to around 150 ATS users and

University staff. That included elevated levels of access, such as the accounts of trainers and athletic directors.

32. That level of access through that number of accounts is an egregious failing of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

33. That access allowed Weiss to download the PHI and personal information belonging to over 150,000 student athletes from over 100 institutions, including the University.

34. On information and belief, the compromised information impacted every University student athlete whose information was saved in the ATS program.

35. From there, Weiss furthered his hack by downloading student athletes' passwords to access the system, using those passwords to breach their personal accounts and download personal, intimate photographs and videos that were not publicly shared.

36. If the University had reasonable cybersecurity measures in place to monitor to monitor the activity on its information systems, it would have caught Weiss' malicious activity.

37. In addition, using information derived from the ATS system, Weiss also breached the social media, email, and/or cloud storage accounts of more than 1,300

additional students and/or alumni from universities and colleges from around the country.

38. The University took no reasonable actions to prevent this access despite its duties to its current and former students.

39. Further, the University also failed to investigate the matter as required under state and federal law. Under Title IX, the University must investigate all instances of sexual harassment against students, including invasions of their privacy on the basis of sex.

40. Weiss preyed on and targeted women during his eight-year breach on the basis of their sex. By failing to protect Plaintiff's PHI, inform her of the extent of the invasion, and take all action necessary under Title IX, the University violated its provisions.

41. To this day, and although the University knew about the breach as early as January 2023, the University has not formally informed class members impacted by Weiss's predation and misconduct.

Plaintiff's Allegations

42. Plaintiff is a former student athlete at the University, having attended the University from 2016 to 2020. While in school, Plaintiff was a member of the swim team while Weiss' breach of the University and Keffer's systems was ongoing.

43. As a University swimmer, Plaintiff received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, treatment plans, and analysis on performance and recovery. Indeed, the PHI includes Plaintiffs' x-rays, appointment details, doctor's notes, and other highly sensitive information that Plaintiff would not have shared had she known the University and Keffer would not protect it.

44. That information was saved by the University and Keffer on Keffer's ATS system.

45. Because the University and Keffer never implemented the security safeguards needed to protect student PHI, Weiss compromised the PHI belonging to every University student whose information was saved in Keffer's ATS database, including, on information and belief, Plaintiff's PHI.

46. This breach of information invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive PHI was stolen by a predator under circumstances the University never should have allowed to exist.

CLASS ALLEGATIONS

47. Plaintiff brings this lawsuit individually and as a class action on behalf of all others similarly situated pursuant to Rule 23.

48. This action satisfies the numerosity, commonality, predominance, typicality and adequacy factors under Rule 23.

49. The Class is defined as:

All individuals whose personal information was accessed and downloaded by Weiss without authorization.

50. **Numerosity.** The class size is estimated to be over 150,000 current and former students from institutions across the country, including the University. That number renders individual joinder impractical.

51. **Commonality and Predominance.** Class members share common factual and legal questions, including whether:

- a. Whether Keffer and the University had duties to safeguard students' information from theft and unauthorized access;
- b. Whether Keffer and the University breached their duties under state and federal law in failing to protect the Class's personal information;
- c. Whether the University was negligent in training and supervising staff in proper data security;
- d. Whether the University was negligent in supervising and monitoring Weiss;
- e. Whether Keffer and the University took reasonable steps to remediate the effects of the data breach;
- f. Whether the breach injured Plaintiff and the Class;

g. Whether Plaintiff and the Class are entitled to damages;

h. Whether this action may be maintained as a class action;

52. All the above questions are common to the class and predominate over any individual questions that may exist.

53. **Adequacy.** Plaintiff will fairly and adequately represent the Class and have retained Counsel experienced and competent in class actions, including data security class actions. Plaintiff and counsel have no conflicts or interests antagonistic to the Class.

54. **Superiority.** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class may be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by defendants' actions. It would otherwise be virtually impossible for class members to seek relief on an individual basis.

CAUSES OF ACTION

COUNT ONE—THE COMPUTER FRAUD AND ABUSE ACT (against Weiss and the University)

55. Plaintiff restates all the allegations above as if set forth below.

56. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

57. He did so in the course of his assigned job responsibilities at the University. Weiss's actions constitute a violation of the Act because he "knowingly accessed a computer without authorization" and/or "exceeded authorized access, thereby obtaining... information." 18 U.S.C. § 1030(a)(2)(C).

58. Under the law, Weiss qualifies as an "inside hacker" since he initially accessed a computer system with legitimate credentials as part of his work with Plaintiff and Class Members in their capacity as student-athletes. However, he then surpassed the scope of his permitted access by entering restricted areas of the digital network.

59. As described above, Weiss's actions were intentional, as he exploited his access and the University's security failures to prey on young women.

60. The University is vicariously liable for his actions because he committed these actions in furtherance of his role as an employee of the University. The University is liable for a completed offenses, including Weiss's.

61. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

62. Plaintiff should be awarded all such forms of damages in this case for Weiss's and the University's willful violation that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT TWO—THE STORED COMMUNICATIONS ACT
(against Weiss and the University)**

63. Plaintiff restates the allegations above as if set forth below.

64. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the intentional access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiff, contain personal, private, and intimate information about and relating to Plaintiff and others situated similar to Plaintiff.

65. Any person who intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

66. Plaintiff's electronic information and communications were in electronic storage and fit directly within the protections of the statute. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his job duties performed for the University.

67. Weiss's access without authorization in connection with his University job duties was intentional and knowingly done.

68. Weiss could not have obtained access without his status as an employee of the University working in the capacity of an athletic trainer with access to the ATS system for which the University employed him.

69. Plaintiff may assert a claim under § 2707 of the Stored Communications Act, for which there is strict liability.

70. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

71. The University's and Weiss's access to Plaintiff's private, personal, and intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a).

72. The University and Weiss knew they did not have authority to access Plaintiff's private, personal, and intimate information, messages, files, and media but accessed it nevertheless.

73. Under the statute, Plaintiff and the Class should be granted the greater of (1) the sum of her actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act. And because the actions were willful, Plaintiff and the Class should be entitled to punitive damages, attorney fees, and costs.

**COUNT THREE—TITLE IX, 20 U.S.C. § 1681(A)
(against the University)**

74. Plaintiff incorporates the allegations above as if set forth below.

75. Title IX states, “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

76. The University receives federal financial assistance for its education program and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

77. Plaintiff is a “person” under the statute.

78. Weiss explicitly targeted and preyed on women when invading their privacy, constituting discrimination on the basis of sex.

79. The University is required under Title IX to investigate allegations of sexual harassment, including Weiss’s misconduct.

80. The University acted with deliberate indifference to Plaintiff’s rights under Title IX by failing to investigate and notify Plaintiff about the incident as required and failing to adequately institute safeguards and protective measures to prevent Weiss from harassing students and invading their privacy.

81. The University’s failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has

effectively denied them equal educational opportunities at the University, including medical care and sports training.

82. At the time the Plaintiff received medical training services from the University, she did not know the University failed to adequately consider her safety including in its engagement, hire, training, and supervision of Weiss.

83. At the time of the University's misconduct and wrongful actions and inactions, Plaintiff was unaware, and or with reasonable diligence could not have been aware, of the University's institutional failings with respect to their responsibilities under Title IX.

84. The University had the ability to prevent the privacy invasion and sexual harassment that harmed Plaintiff and the Class.

85. Plaintiff and the Class should be awarded all such forms of damages in this case that the University's misconduct caused, including damages, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT FOUR—THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“STATE CREATED DANGER”
(against the University)**

86. Plaintiff repeats all allegations above as if set forth below.

87. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

88. The University recklessly exposed Plaintiff to a dangerous predator, Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

89. Plaintiff as a female student athlete was a foreseeable victim.

90. The invasion of Plaintiff's privacy was foreseeable. The decisions and actions to deprive Plaintiff of a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

91. The University acted in willful disregard for the safety of Plaintiff. The decisions and actions to deprive Plaintiff a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

92. The University acted in willful disregard for the safety of Plaintiff.

93. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT FIVE –THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“FAILURE TO TRAIN AND SUPERVISE”
(against the University)**

94. Plaintiff repeats all allegations above as if set forth below.

95. The University had the ultimate responsibility and authority to train and supervise its employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

96. The University failed to train and supervise its employees, agents, and/or representatives including all faculty and staff, regarding the following duties: Perceive, understand, and prevent inappropriate sexual harassment on campus; Perceive, report, and prevent inappropriate invasion of privacy campus; Provide diligent supervision to and over student athletes and other individuals, including Weiss; Thoroughly investigate any invasion of privacy by Weiss; Ensure the safety of all students, faculty, staff, and visitors to the University's campuses and premises; Provide a safe environment for all students, faculty, staff, and visitors to the University's premises free from sexual harassment; Properly train faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

97. The University failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiff's rights.

98. The University's failure to adequately train was the result of its deliberate indifference toward the well-being of student athletes.

99. As a result, the University deprived Plaintiff of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

100. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT SIX—BREACH OF IMPLIED CONTRACT
(against the University and Keffer)**

101. Plaintiff repeats all allegations above as if set forth below.

102. Keffer and the University impliedly promised to safeguard Plaintiff and the Class's sensitive information when collecting it through the ATS program.

103. Those promises include those in Keffer's privacy policy and the University's school policy.

104. Plaintiff would not have provided her information to the University and Keffer had she known it would not adequately protect it.

105. Plaintiff and the Class provided value to Keffer and the University through direct and indirect means, including through their tuition payments, which the University used in part to secure Keffer's services, and the value of their data to University and Keffer.

106. The University and Keffer both broke their promises to protect Plaintiff and the Class's sensitive information when they failed to implement the basic security safeguards needed to fulfill those promises.

107. That breach caused Plaintiff and the Class contract damages, as they have been deprived of the benefit of their bargain.

**COUNT SEVEN—NEGLIGENCE & NEGLIGENCE PER SE
(against Keffer Only)**

108. Plaintiff realleges all previous paragraphs as if fully set forth below.

109. Plaintiff and members of the Class entrusted their PHI to Keffer. Keffer owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

110. Keffer owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Keffer's failure to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI—just like the breach that ultimately came to pass. Keffer acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's PHI by disclosing and providing access to this information to third parties and by failing to properly

supervise both the way the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Keffer owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI. Keffer also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the breach.

112. Keffer owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Keffer's inadequate security protocols. Keffer actively sought and obtained Plaintiff's and members of the Class's personal information and PHI.

113. The risk that unauthorized persons would attempt to gain access to the PHI and misuse it was foreseeable. Given that Keffer holds vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Keffer's databases containing the PHI.

114. Keffer's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

115. In addition, Keffer owed a duty of care to Plaintiff and the Class under HIPAA. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

116. The breach here resulted from multiple failures by Keffer to implement adequate security, including:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only

to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

117. These regulations were intended to protect the Class at issue here, and Keffer's failure to abide by them caused Plaintiff and the Class damages.

**COUNT EIGHT—INVASION OF PRIVACY
“Intrusion Upon Seclusion”
(against Weiss)**

118. Plaintiff realleges all allegations above as if fully set forth below.

119. Plaintiff and the Class's PHI was stored electronically and were intended to remain private.

120. Indeed, Plaintiff reasonable expected that information would remain private under the University and Keffer's policies.

121. Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff.

122. His actions were unauthorized, and the invasion would be highly offensive to any reasonable person.

123. Plaintiff and the Class never granted permission for this access and Weiss's intrusion is a severe violation of their privacy, causing them severe emotional damages.

WHEREFORE, Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- b. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- c. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- d. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI and PII;
- e. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

- f. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- g. Awarding attorneys' fees and costs, as allowed by law;
- h. Awarding prejudgment and post-judgment interest, as provided by law;
- i. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- j. Granting such other or further relief as may be appropriate under the circumstances.

Dated: April 2, 2025

Respectfully submitted,

/s/ David H. Fink
David H. Fink (P28235)
Nathan J. Fink (P75185)
FINK BRESSACK
38500 Woodward Ave., Suite 3500
Bloomfield Hills, MI 48304
Tel: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

J. Gerard Stranch, IV
Grayson Wells (application for admission to
be submitted)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwellis@stranchlaw.com